TCP/IP für Anfänger

Chaos Communication Congress
Berlin, 27.-29. Dezember 1998

Übersicht

- **TCP/IP und das Internet**
- Protokolle
  - Schichtenmodell
  - IP, UDP, TCP, ARP
- Routing und Congestion Control
- Anwendungen
- Angriffspunkte

TCP/IP und das Internet

- hardware-unabhängig
- Entwicklung seit 1983 (DARPA)
- keine zentrale Verwaltung
- kein zentraler Knoten (im Gegensatz zu SNA)
- Ausfallsicherheit als Designziel (DOD)
- Routing Paket-per-Paket

TCP/IP und das Internet

- Applikationsunabhängig
- Standards: "RFC" (Request for Comment), numeriert - auf vielen Servern verfügbar, z.B. ftp://rtfm.mit.edu
- Auch auf der Chaos-CD enthalten
- Im Gegensatz zu den ISO/OSI-Protokollen kein "offizieller" Standard, aber weithin akzeptiert

Übersicht

- TCP/IP und das Internet
- **Protokolle**
  - **Schichtenmodell**
  - **IP, UDP, TCP, ARP**
- Routing und Congestion Control
- Anwendungen
- Angriffspunkte

Protokolle

- Paketorientiert
- Schichtenmodell
- Adressierung

Schichtenmodell

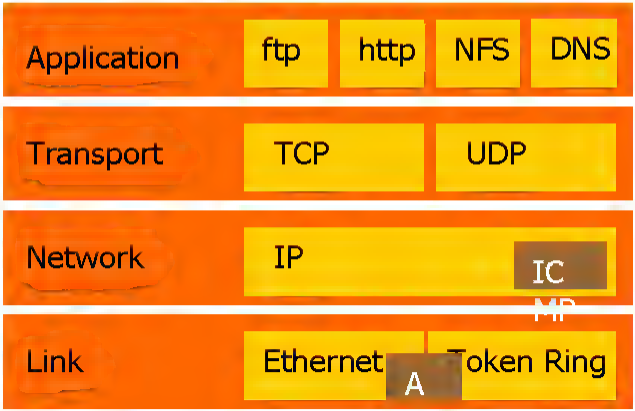
Application: Benutzerprozesse

Transport: Paketsicherung

Network: Paketzustellung, Routing

Link: Hardware, Gerätetreiber

Schichtenmodell



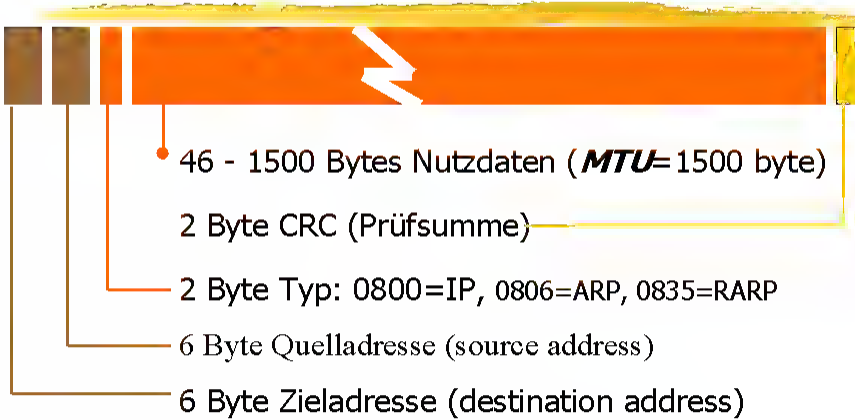
Link Layer

- Ethernet
- Token Ring
- HDLC (für WAN)
- ISDN
- usw.

Ethernet

- 10 oder 100 Mbit/s: Gleiches Protokoll
- Frame-Typ: Ethernet-II
- 6 Byte Adressen, weltweit eindeutig (in der Hardware festgelegt)
- CSMA/CD, "Shared media", nicht kollisionsfrei, stochastisches Verhalten
- Neuerdings auch "switched Ethernet", kollisionsfrei (gleiches Protokoll)

Ethernet (RFC894)



Der Datenteil muß notfalls auf 46 Bytes aufgefüllt werden.

Exkurs: Ethernet-Kabel

10Base-2, Cheapernet

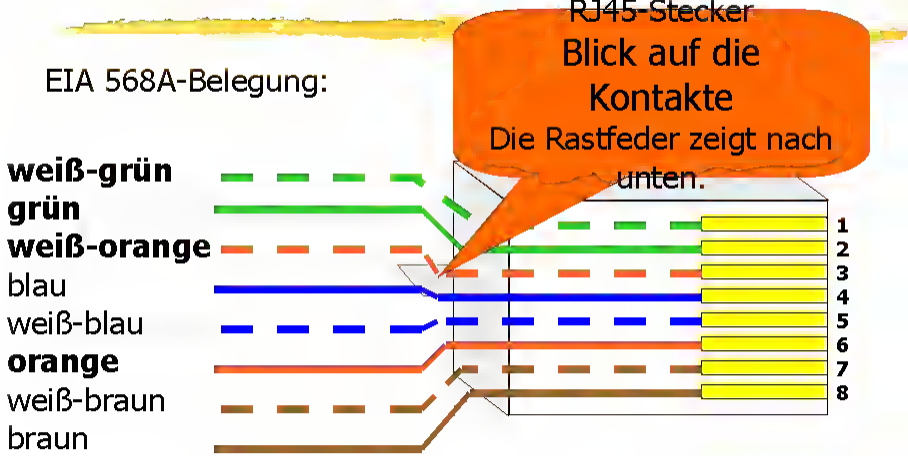
- Koaxial
- RG58 Kabel, 50 Ohm
- Bus-Verkabelung, T-Stücke
- Kabel muß mit je 50 Ohm terminiert sein
- Max 185 m / Segment
- 10 Mbit/s

10Base-T usw.

- Verdrillte Paare
- EIA568 Cat.3/4/5
  4 Adernpaare (2 genutzt)
- Stern-Verkabelung vom Hub
- Max. 90+10 m/Strang
- fehlertoleranter
- 10 und 100 Mbit/s

Exkurs: RJ45-Stecker

EIA 568A-Belegung:



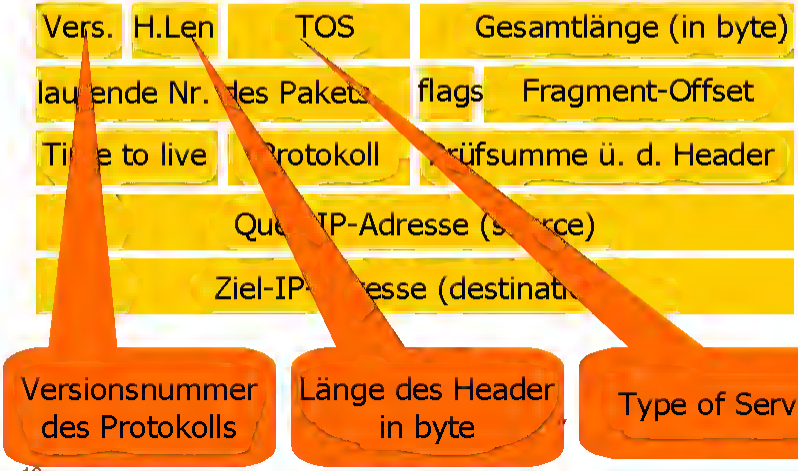
IP - Internet Protocol

- Paketvermittelnd
- Ungesichert
- verbindungslos
- 32 bit Adressen, meist als 1.2.3.4 (dezimal) geschrieben

IP - Adressen

- Eine Adresse gehört jeweils zu einem Interface. D.h. ein Rechner mit mehreren Netzwerkkarten hat auch mehrere Adressen.
- Wenn Daten zu groß für den nächsten Hop, werden sie zerlegt (fragmentiert)
- Mehr Details später

IP Paketaufbau



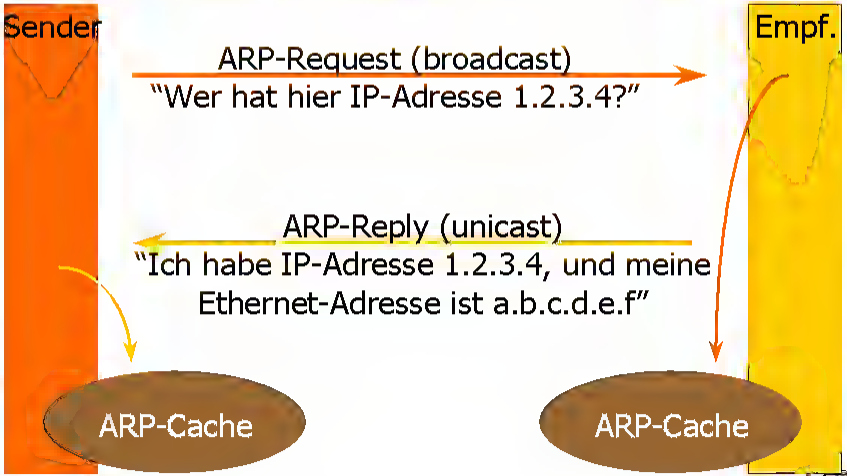
ICMP: Internet Control Message Protocol

- Für Status- und Fehlermeldungen
- "host unreachable"
- "network unreachable"
- PING nutzt ICMP echo request/reply
- Teil von IP (network layer), nutzt aber IP-Pakete zur Datenübertragung

ARP: Address Resolution Protocol

- Zur Zustellung von IP-Paketen im LAN wird die physische (z.B. Ethernet-) Adresse benötigt
- Ethernet-Adressen (48 bit) sind weltweit eindeutig in der Hardware "eingebrannt"
- Logische IP-Adressen (32 bit) sind vom Netzverwalter festgelegt
- ARP erlaubt Umsetzung

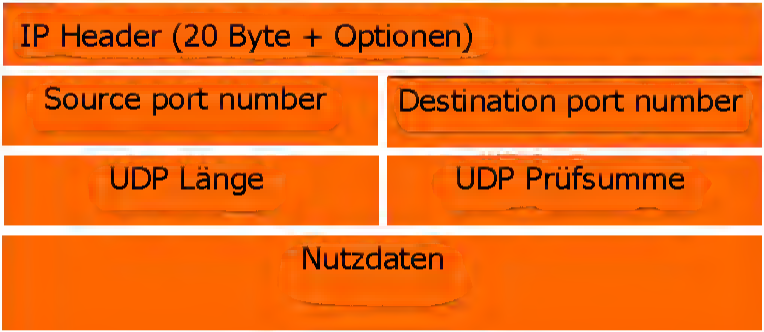
ARP


Sender
Empf.
ARP-Request (broadcast)
"Wer hat hier IP-Adresse 1.2.3.4?"
ARP-Reply (unicast)
"Ich habe IP-Adresse 1.2.3.4, und meine Ethernet-Adresse ist a.b.c.d.e.f"
ARP-Cache
ARP-Cache

UDP - User Datagram Protocol

- Simpelstes Internet-Protokoll auf Transportebene (Ebene 3)
- Verbindungslos
- Ungesichert - "fire and forget"
- Anwendungen: z.B. DNS, NFS
- Zusätzlich zum 20 Byte IP-Header noch zwei 16 bit Portnummern, 16 bit Länge und eine 16 bit Prüfsumme

UDP Paketaufbau



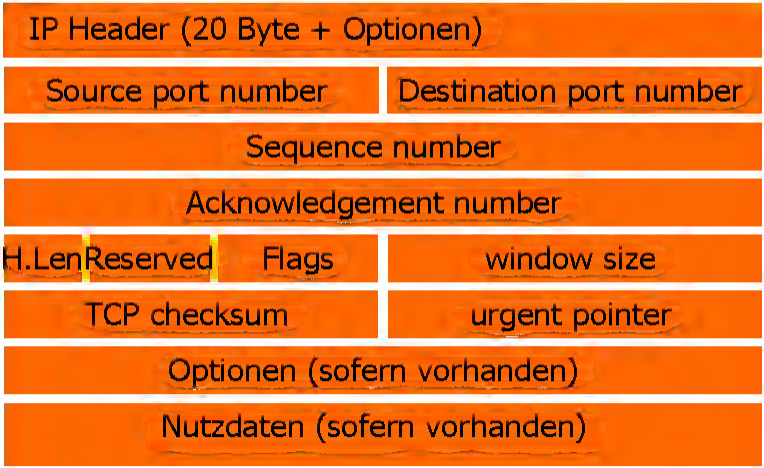
Ports

- UDP und TCP verwenden "Ports" als Erweiterung der IP-Adresse.
- Eine Datenübertragung ist durch 4 Adressen gekennzeichnet:
  - Quell-Adresse, Quell-Port
  - Ziel-Adresse, Ziel-Port
- Ports beschreiben einen Prozess auf einem Rechner

TCP: Transmission Control Protocol

- Verbindungsorientiert (wie Telefon)
- gesicherte Verbindung: Alles kommt an, in der richtigen Reihenfolge, und nicht doppelt
- die meisten Internet-Anwendungen verwenden TCP
- Weitaus komplexer als UDP
- Client-Server Modell üblich
- Versucht, Netzüberlast zu vermeiden

TCP Paketaufbau



TCP - Sequence / Ack number

- Sequence number:
  - Nummer des ersten Bytes in diesem Segment (Flags zählen mit)
- Acknowledgement number:
  - Die Sequence number, die als nächste erwartet wird

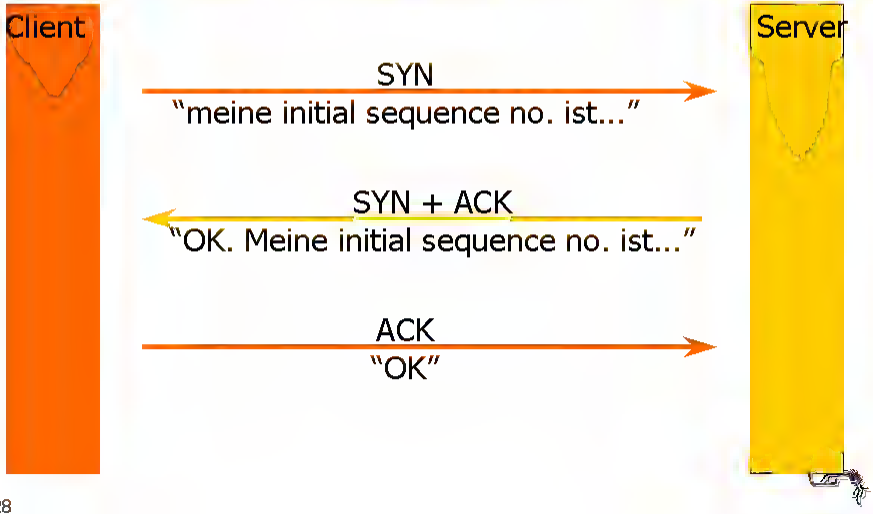
TCP - Flags

- URG - urgent pointer ist gültig
- ACK - acknowledgement number ist gültig
- PSH - Empfänger soll sofort verarbeiten (push)
- RST - Reset der Verbindung
- SYN - Verbindungsaufbau
- FIN - Verbindungsabbau

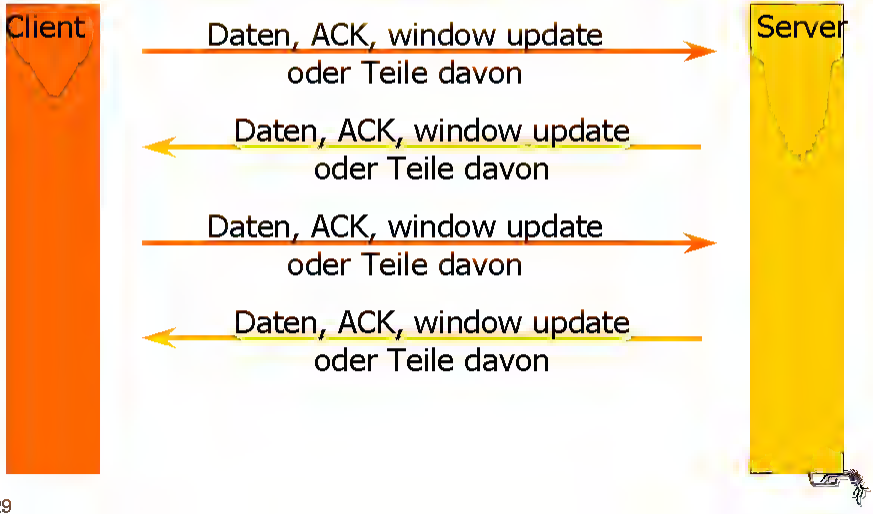
TCP - Window size

- Window size:
  - Der Empfänger bestimmt, wieviel Daten er noch aufnehmen will (z.B. Puffergröße)
  - Wenn der Empfänger (wieder) mehr Daten verarbeiten kann, sendet er ein "Window update"
  - Bei Window size 0 kann nichts mehr gesendet werden, bis der Empfänger sein Window wieder öffnet (window update)

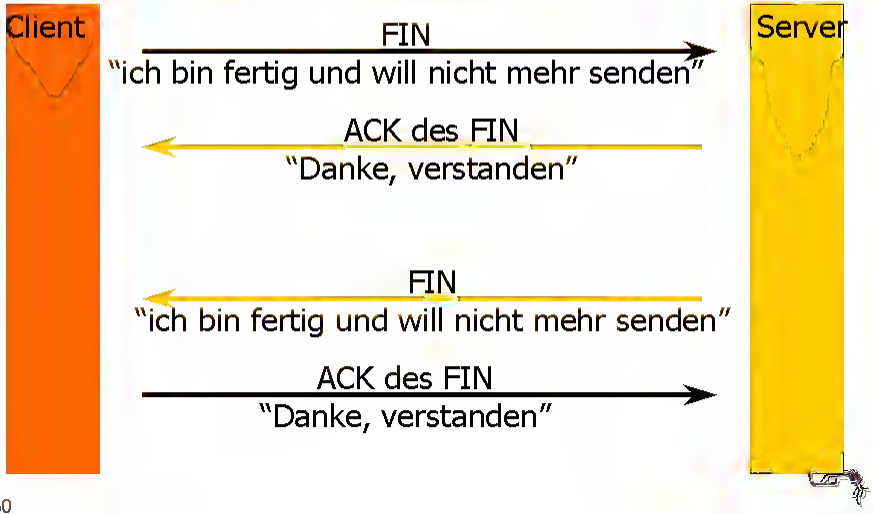
TCP - Verbindungsaufbau



TCP - Verbindung steht



TCP - Verbindungsabbau



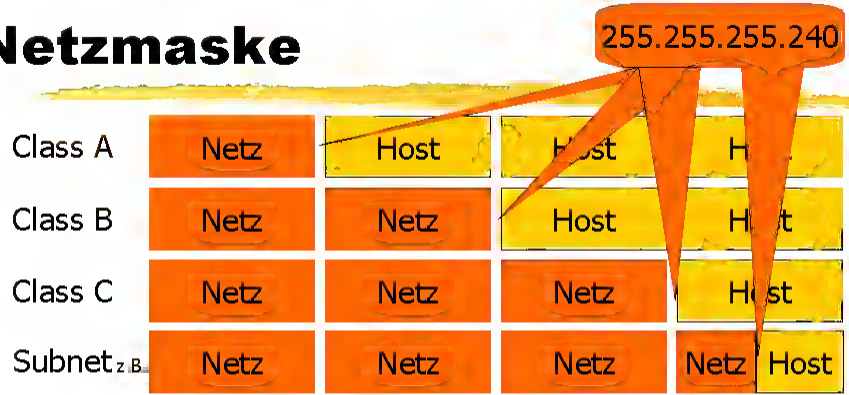
Übersicht

- TCP/IP und das Internet
- Protokolle
  - Schichtenmodell
  - IP, UDP, TCP, ARP
- **Routing und Congestion Control**
- Anwendungen
- Angriffspunkte

Routing

- IP-Adressen sind 32 bit organisiert.
- Es gibt Class-A, Class-B und Class-C Netze. Diese unterscheiden sich durch die Netzmaske, die angibt, welcher Teil der Adresse das Netz und welcher den Rechner innerhalb des Netzes bezeichnet.
- Routing-Entscheidungen werden nur nach dem Netz-Teil der Adresse getroffen!

Netzmaske



Es gibt nur wenige Class B und noch weniger Class A Netze.
Class C-Netze, oder Blöcke davon, sind das Übliche.
Die Klassen wurden eingeführt, um die Tabellen in den Routern klein zu halten.
Es ist möglich, die Netzmaske unabhängig von der Klasse frei zu setzen, um ein Netz weiter zu unterteilen (subnetting)

Netzmaske

Adresse	192. 168. 153. 23
Netzmaske	255. 255. 255. 240
Adresse & Netzmaske (bitweises UND)	192. 168. 153. 16
Netz-Teil der Adresse	192. 168. 153. 16
Host-Teil der Adresse	0. 0. 0. 7

Routing-Ablauf

- Aufspalten der Zieladresse in Netz- und Host-Teil (durch AND mit der Netzmaske)
- Durchsuchen der Routing-Tabelle nach dem errechneten Netzteil
- Wenn gefunden: An das in der Tabelle eingetragene Interface senden (next hop)
- Sonst: Zur Default-Route, falls vorhanden
- Ansonsten: ICMP "Network unreachable"

Routing-Protokolle

- Routing-Protokolle dienen dazu, die Routingtabellen automatisch zu pflegen, wenn z.B. Wege unpassierbar werden
- Es gibt verschiedene Protokolle
  - RIP: Fuer LAN geeignet, viel Traffic
  - EGP, BGP: Fuer WAN / ASN zu ASN
- Unter UNIX in routed (nur RIP) bzw. gated implementiert

Nameserver

- Für Menschen sind numerische Adressen schwer merkbar
- Daher sorgt das DNS (Domain Name System) dafür, daß leichter merkbare Namen verwendet werden können
- Nameserver bilden eine weltweit verteilte Datenbank

Nameserver

- Die Namen sind hierarchisch organisiert, z.B.

  blackbox.congress.ccc.de
- Eine Anfrage fragt nach
  - de? Deutschland! ➔ ns.nic.de
  - ccc.de? Chaos! ➔ ns.ccc.de
  - congress.ccc.de? ➔ ns.congress.ccc.de
  - Resultat: 195.21.208.23

Vermeidung von Überlast

- Wenn das Netz an einer Stelle stark belastet ist (z.B. Übergang vom LAN ins langsamere WAN), gehen Pakete verloren.
- Wenn nun der Sender weiter mit voller Kapazität sendet, wird die Situation nur schlimmer.

Vermeidung von Überlast

- TCP hat zwei Mechanismen zur Vermeidung von Überlast: Slow Start und Congestion Avoidance.

Slow Start

- Eine TCP-Verbindung beginnt nicht, mit der Window-Größe zu senden, die die Gegenseite annonciert, sondern sendet zunächst nur ein Segment.
- Die effektive Window-Groesse wird nun mit jedem eingetroffenen ACK um ein weiteres Segment erhöht, bis die Windowgröße erreicht ist.

Congestion Avoidance

- Wenn zwischendurch Pakete verlorengehen (erkennbar daran, daß doppelte ACK-Nachrichten eintreffen), wird das fehlende Paket erneut gesendet (retransmit).
- Die Datenrate wird dann vermindert und steigt langsam wieder an.

Übersicht

- TCP/IP und das Internet
- Protokolle
  - Schichtenmodell
  - IP, UDP, TCP, ARP
- Routing und Congestion Control
- **Anwendungen**
- Angriffspunkte

Anwendungen

- Die meisten Anwendungen basieren auf TCP, nur wenige auf UDP.
- UDP-basierend sind NFS (Network File System) und DNS.

UDP-Anwendungen

- NFS: Network File System, entwickelt von Sun.
  Relativ langsam, aber extrem stabil. Das Protokoll ist "stateless", d.h. alle Statusinformation liegt nur auf dem Client. Der Server kann zwischendurch neu starten, ohne daß der Client dies normalerweise merkt.
  NFS Version 2 kann auch TCP verwenden

UDP-Anwendungen

- DNS: Domain Name system
  Clients fragen über UDP bei den Name Servern an.
  Die Server antworten ihrerseits per UDP.
- Traceroute: Feststellen, wie meine Daten zum Empfänger kommen.
  Nur aktuelles Bild, das nächste Paket kann schon einen anderen Weg nehmen.

TCP-Anwendungen

- Telnet: Terminal-Emulation, login
- SSH: Das "bessere Telnet", verschlüsselt
- FTP: Dateitransfer
- HTTP: Übertragungsprotokoll des WWW
- SMTP, POP3: Electronic Mail
- usw.

Übersicht

- TCP/IP und das Internet
- Protokolle
  - Schichtenmodell
  - IP, UDP, TCP, ARP
- Routing und Congestion Control
- Anwendungen
- **Angriffspunkte**

Angriffspunkte

Dieses Thema bildet einen besonderen Schwerpunkt morgen.

Daher hier nur ein knapper Überblick.

Angriffspunkte

- Denial of Service: Berechtigte Nutzer können nicht arbeiten
- Ausspähen von Daten durch passives Mitlesen
- Verfälschen von Daten unterwegs
- Aktiver Eingriff in Netzknoten (Rechner, Router)
- IP Spoofing

Denial of Service

- Flood ping usw.: Überlasten eines Netzes oder Rechners
- Ping mit zu großen Paketen
- SYN-flooding
- Illegale Fragmente
- Beruht meist auf Fehlern in der IP-Implementierung des angegriffenen Systems

Ausspähen von Daten

- Mitlesen (Sniffer) im LAN
  - Bei Ethernet einfach
  - Zur Fehleranalyse oder Spionage
  - etherfind, tcpdump, RMON-Probe
- Mitlesen in WAN-Zwischenstationen, z.B. beim Internet-Provider
- Log-Dateien, z.B. WWW Proxy

Einschleusen von Daten

- Einschleusen anderer Daten (unter falscher Identität)
- Übernahme (hijacking) bestehender Verbindungen, z.B. juggernaut
- Oft bei applikationsspezifischen Client-Server-Systemen, z.B. Datenbanken

IP Spoofing

- Setzen der Quell-Adresse im IP-Header auf eine andere Adresse
- Oft eine Adresse im angegriffenen LAN
- Basis für weitere Attacken
- Keine Antwort möglich
- Einfache Protokolle, wie SMTP, funktionieren auch ohne Antwort (Antwort vorhersehbar) -> E-Mail Spam

Literatur

- W.Richard Stevens, TCP/IP Illustrated, Addison-Wesley (besonders Vol.1)
- Olaf Kirch, Linux Network Administrators Guide, LDP bzw. O'Reilly
- Douglas Comer, Internetworking with TCP/IP, Prentice-Hall
- RFCs